



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/640,839	08/16/2000	Mark Gregory McClanahan	RPS9-2000-0052US1	4229
45211	7590	11/28/2005		
KELLY K. KORDZIK WINSTEAD SECHREST & MINICK PC PO BOX 50784 DALLAS, TX 75201				
EXAMINER LANIER, BENJAMIN E				
ART UNIT 2132		PAPER NUMBER		

DATE MAILED: 11/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**MAILED**

NOV 25 2005

Technology Center 2100



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents  
United States Patent and Trademark Office  
P.O. Box 1450  
Alexandria, VA 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

**BEFORE THE BOARD OF PATENT APPEALS  
AND INTERFERENCES**

Application Number: 09/640,839

Filing Date: August 16, 2000

Appellant(s): MCCLANAHAN, MARK GREGORY

\_\_\_\_\_  
Robert A. Voigt, Jr.  
For Appellant

**EXAMINER'S ANSWER**

This is in response to the appeal brief filed 22 September appealing from the Office  
action mailed 01 July 2005

**(1) Real Party in Interest**

A statement identifying by name the real party in interest is contained in the brief.

**(2) Related Appeals and Interferences**

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

**(3) Status of Claims**

The statement of the status of claims contained in the brief is correct.

**(4) Status of Amendments After Final**

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

**(5) Summary of Claimed Subject Matter**

The summary of claimed subject matter contained in the brief is correct.

**(6) Grounds of Rejection to be Reviewed on Appeal**

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

**(7) Claims Appendix**

The copy of the appealed claims contained in the Appendix to the brief is correct.

**(8) Evidence Relied Upon**

5,944,824                                      HE                                      8-1999

**(9) Grounds of Rejection**

The following ground(s) of rejection are applicable to the appealed claims:

*Claim Rejections - 35 USC § 102*

Art Unit: 2132

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-8, 10-13, 15-20, 22, 23, 28-35, 37-40, 42-47, 49, 50, 55-62, 64-67, 69-74 76, 77, are rejected under 35 U.S.C. 102(e) as being anticipated by He, U.S. Patent No. 5,944,824. Referring to claims 1, 7, 28, 33, 55, 60, He discloses a system for single sign-on to a plurality of network elements wherein users are allowed to log-on only once at a user station and a Security Server will automatically log the user on to all the network elements that the user is authorized to access (Col. 2, lines 25-32). The architecture and method for the Single Sign-on system (“SSO”) meets the limitation of providing an application framework. The SSO allowing the user to log-on to the system meets the limitations of generating an application framework sign-on screen, wherein said application framework logs on a user, and entering a logon input on said generated application framework sign-on screen. The user accessing network elements that the user is authorized to access and the database for user authorization and user privilege control (Fig. 2) meet the limitation of user log-on with a first level of access in said underlying operating system. When the user attempts to log-on the information entered by the user is checked against the information in the user profile of the central security database at the security server and assures that the user accesses the correct network elements based on the user privilege (Col. 5, lines 8-15), which meets the limitation of comparing said logon input with an application framework security database to determine level of access. The SSO system is incorporated with the security

Art Unit: 2132

server (Figs. 1 & 2), which meets the limitation of a processor, a memory unit operable for storing a computer program operable for bypassing an initial sign-on screen of an underlying operating system with a single sign capability, an input mechanism, an output mechanism, and a bus system coupling the processor to the memory unit, input mechanism, and output mechanism.

Referring to claims 2, 3, 18, 29, 30, 45, 56, 57, 72, He discloses that the user attempts to log-on the information entered by the user is checked against the information in the user profile of the central security database at the security server and assures that the user accesses the correct network elements based on the user privilege (Col. 5, lines 8-15), which meets the limitations of selecting an indication of said first level of access, the user is logged onto said underlying operating system and an application environment with said first level of access thereby bypassing said initial sing-on screen of said underlying operating system with said single sign-on.

Referring to claims 4, 10, 16, 24, 31, 37, 43, 51, 58, 64, 70, 78, He discloses that the user privilege level determines the access rights that the user has and what network elements the user can access (Col. 5, lines 41-45). Unless the user is granted additional access rights (Col. 5, lines 45-48 & Col. 8, lines 40-65), the user can only access the network elements designated to that user as being authorized for their use, and attempted accesses of unauthorized network elements will be rejected and logged (Col. 5, lines 49-58), which meets the limitation of if said logon input is not entitled to a second level of access according to said application framework security database, then said user is logged onto an application environment and said underlying operating system as said first level of access.

Referring to claim 5, 23, 32, 50, 59, 77, He discloses that the user log-on information is a user ID and password (Col. 2, lines 60-61).

Referring to claim 6, 17, 19, 22, 25, 34, 44, 46, 49, 52, 61, 71, 73, 76, 79, He discloses that if a user log-on gives the user “super user” access rights then the user is provided with more privileges to perform administrative functions in a network element (Col. 8, lines 51-54), which meets the limitation of executing a switch user program to switch said user to said second level of access.

Referring to claims 8, 13, 20, 26, 35, 40, 47, 53, 62, 67, 74, 80, He discloses that the user records, stored in registry (Col. 15, lines 52-53), are modified to give the user more access rights (Col. 5, lines 41-48), which meets the limitation of a user switching program switches said user to said second level of access by modifying an underlying operating system’s registry.

Referring claims 11, 12, 15, 38, 39, 42, 65, 66, 69, He discloses that the SSO contains an indication digit for regular users and for super users (Col. 10, line 58 – Col. 11, line 10), which meets the limitation of if said logon input is entitled to a second level of access according to said application framework security database, then the method further comprises the step of generating an indication of said second level of access, executing a switch user program to switch level of access to said second level of access by selecting said indication of said second level of access.

#### **(10) Response to Argument**

Applicant’s assertion that one having ordinary skill in the art can determine the scope of the claimed subject matter in claims 9, 14, 21, 27, 36, 41, 48, 54, 63, 68, 75, and 81 is not persuasive because the claims require clarification so that one having ordinary skill in the art can

Art Unit: 2132

determine the scope. Taking claim 9 for example, the claim language requires logging off a user with a first level of access and then logging on said user with a second level of access. This limitation renders the claims vague and indefinite because the claim from which claim 9 depends (Claim 8), claims that a switch program switches said user to said second level of access by modifying an underlying operating system's registry. There is no claim limitation requiring logging on or logging off in claim 8. A simple claim amendment to the claims specifying that the user is switched to said second level of access would have overcome the 112 rejections.

Applicant appears to be arguing for all 9 claim groupings that the He reference does not disclose an application framework and an underlying operating system to perform the claimed limitations. Applicant has not provided an explanation in the arguments of how their claimed application framework or underlying operating system differs from the He reference. Applicant appears to be relying on features from the specification to differentiate the claims from the He reference, but have failed to point to any such features in the specification. Applicant should bear in mind that although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). As stated in previous office actions, using a reasonable interpretation in the art an application framework is merely computer software. Applicant points to page 7, lines 27-28 to define Applicant's application framework. The specification defines an application framework as controlling what applications are accessible to the particular user. He discloses that the security mechanism (Figure 2, element 32) that is included in the security server (Figure 2, element 15), that performs the single sign-on capabilities and user authentication, is computer software (Col. 7, lines 7-9). The security server logs the user on to all the network elements that the user is

Art Unit: 2132

authorized to access. Therefore, using a broad but reasonable interpretation of application framework, and Applicant's definition of an application framework in the specification, the claim limitations are met by the He reference. He also inherently discloses an underlying operating system because one having ordinary skill in the art would recognize that a computer system having user privilege controls (Figure 2, element 58) would be running on an underlying operating system.

To exemplify how the He reference meets the claim limitations we will look at independent claim 1. He discloses a system for single sign-on to a plurality of network elements wherein users are allowed to log-on only once at a user station and a security server, in turn, will automatically log the user on to all the network elements that the user is authorized to access (Col. 2, lines 25-32), which meets the limitation of providing an application framework, wherein said application framework logs on a user with a first level of access in said underlying operating system. The application framework and underlying operating system limitations are met in light of the previous paragraph. The single sign-on allows the user to log-on only once at a user station (Figure 1, element 14) for authentication by the security server (Figure 1, element 15 & Col. 2, lines 25-32). The network authentication module (Figure 2, element 50) of the security server sends a request to the user station requesting a user identifier and a password (Col. 5, lines 7-9), which meets the limitation of generating an application framework sign-on screen because the user will see the received request on the monitor of the user station (Figure 1, element 14). The user will then enter the requested user identifier and password, which will be checked against the information in the user profile of the central security database of the security server (Col. 5, lines 9-11), which meets the limitation of entering a login input on said generated application



Art Unit: 2132

framework sign-on screen. The authorization module (Figure 2, element 52) of the security server determines the set of network elements that the authenticated user can access based on the log-on information provided by the user (Col. 5, lines 11-19), which meets the limitation of comparing said logon input with an application framework security database to determine level of access. He discloses normal users and super users (Col. 8, lines 40-65) and the ability to change or update the user privileges (Col. 5, lines 41-49), which meets the limitation of different levels of access and the ability to change the access levels.

**(11) Related Proceeding(s) Appendix**

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

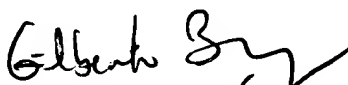
Benjamin E. Lanier



Conferees:

Gilberto Barron

Christopher Revak (Primary <sup>2131</sup>)



GILBERTO BARRÓN  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100